IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

|  |  |  |
|---|---|---|
| KAJEET, INC. | § |  |
|  | § |  |
| Plaintiff, | § | C.A. 21-cv-5-MN |
|  | § |  |
| v. | § | **JURY TRIAL DEMANDED** |
|  | § |  |
| MCAFEE CORP. | § |  |
|  | § |  |
| Defendant. | § |  |

## PLAINTIFF'S BRIEF IN OPPOSITION TO DEFENDANT'S MOTION FOR SANCTIONS UNDER RULE 11

Dated: September 7, 2021

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
FARNAN LLP
919 N. Market Str., 12th Floor
Wilmington, DE 19801
Tel: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

*Attorneys for Plaintiff Kajeet, Inc.*

Of Counsel:

Jonathan T. Suder
Michael T. Cooke
Corby R. Vowell
Richard A. Wojcio, Jr.
FRIEDMAN, SUDER & COOKE
Tindall Square Warehouse No. 1
604 East 4th Street, Suite 200
Fort Worth, Texas 76102
Telephone: (817) 334-0400
Facsimile: (817) 334-0401
jts@fsclaw.com
mtc@fsclaw.com
vowell@fsclaw.com
wojcio@fsclaw.com

# Table of Contents

## TABLE OF AUTHORITIES

## I. NATURE AND STAGE OF THE PROCEEDINGS

Plaintiff Kajeet, Inc. ("Plaintiff" or "Kajeet") files this Brief in Opposition to McAfee Corp.'s ("Defendant" or "McAfee") Motion for Sanctions Under Rule 11. For the following reasons, the Court should deny McAfee's Motion in its entirety. After a thorough investigation of the McAfee products accused of infringement in this case, Kajeet filed its Original Complaint on January 24, 2021 for infringement of at least claims 1 and 27 of the '559 patent. On March 29, 2021, McAfee moved to dismiss the Original Complaint asserting that Kajeet had not met the pleading requirements for direct and indirect infringement.

Out of an abundance of caution and to conform to the Order of this Court from another matter against Gryphon Online Safety, Inc., Kajeet filed its First Amended Complaint ("FAC") in this case on April 12, 2021. *See Kajeet, Inc. v. Gryphon Online Safety, Inc.*, Case No. 19-cv-2370-MN. In the FAC, Kajeet restated its detailed basis for infringement set forth in the Original Complaint and also included a claim chart mapping the factual allegations about the design and operation of McAfee's products to specific elements of the asserted claims as well as including links to product literature describing the operation of the accused products. On April 26, 2021, McAfee filed another Motion to Dismiss challenging the sufficiency of the allegations in Kajeet's FAC. That Motion has been fully briefed and is still pending before the Court. Subsequently, on July 30, 2021, McAfee served its Rule 11 Motion on Kajeet which was then filed on August 23, 2021.

## II. SUMMARY OF THE ARGUMENT

There is nothing in McAfee's Motion that shows Kajeet in any way violated Rule 11 by bringing this suit or continuing forward with the litigation. In stark contrast to McAfee's Motion, Kajeet provides considerable evidence in this Opposition that not only its pre-suit investigation was thorough and sound but also that its infringement theory continues to be viable at this stage of the case.

First of all, the Motion is premature – a fact that McAfee recognized when objecting to Kajeet's interrogatories seeking information relevant to the issues presented here.[1] McAfee has deliberately filed its Motion now to circumvent the entire disclosure process that this Court has adopted to govern patent cases, which includes orderly disclosure of technical document production, exchange of infringement and validity contentions, claim construction, and expert disclosure. The case is currently in its early stages and very little discovery has taken place. McAfee produced only a few pages of technical documents as its purported "core technical documents" and has refused to produce its other technical documents already requested by Kajeet until about 4-6 weeks from now. In fact, McAfee served a copy of this Motion under the 21-day safe harbor provision prior to receiving Kajeet's Disclosure of Initial Claim Charts (infringement contentions).

McAfee's refusal to produce the bulk of its technical information now is particularly telling given that it chose not to include any actual evidence in its Motion regarding how its products work. Instead, McAfee relies on mere attorney argument to request that this Court dismiss this case with prejudice. Notably, McAfee does not cite to any technical documentation describing the design, structure, or operation of its products. Nor does McAfee provide a declaration from one of its engineers or other employees to support its non-infringement positions. Almost all of the evidence regarding how McAfee's products work is in McAfee's possession, yet it elected not to provide any of this evidence to the Court. Further, McAfee did not provide a declaration from a

[1] When requested to disclose its noninfringement position(s) and bases therefore, McAfee objected to the request as being premature. *Infra*, p.6.

technical expert that has tested or reviewed documentation regarding the accused products. Likewise, McAfee has not cited at all to its source code which it contends is the most relevant information to the infringement issues in the case.

As the evidence presented in this Opposition shows, Kajeet's pre-suit investigation was more than sufficient and included a detailed review of the relevant publicly available information. Kajeet has litigated the patent-in-suit in prior litigations and applied the claims consistently to the accused products in this case to determine that McAfee's products infringed. After McAfee informally raised its current non-infringement positions, Kajeet had its technical expert, Mr. Chetan Sharma, reviewed these positions in light of the publicly available information and information available from McAfee to date. As set forth below, Mr. Sharma tested the accused products extensively to aid his understanding of their operation. He also used a network protocol analyzer, Wireshark, to observe the communications between devices operating McAfee's software. In addition, he performed an initial review of McAfee's source code. Through this review and testing, Mr. Sharma's reached conclusions that support Kajeet's infringement theory.

McAfee simply cannot show that Kajeet violated Rule 11 by filing this lawsuit or continuing to litigate its case in light of the information available to Kajeet to date that confirms its infringement position.

McAfee's three previous motions have not resulted in dismissal of this case. Clearly dissatisfied, McAfee has now upped the ante by moving for sanctions, not to mention attempting to disrupt the case's progression. McAfee hopes, at best, to obtain dismissal before providing Kajeet the benefit of fulsome discovery or claim construction, and at worst force Kajeet to disclose expert opinions that McAfee would never otherwise receive at this early stage. Kajeet has filed nineteen lawsuits - some of which involved similar accused features as McAfee - and resolved twelve of them. That no other defendant has filed a Rule 11 motion speaks volumes about McAfee's latest ploy.

## III. STATEMENT OF FACTS

Kajeet's efforts and ingenuity have yielded thirty-eight U.S. Patents, many of which involve the same or similar technology as the claims of the asserted patent in this case. In order to protect its intellectual property rights, Kajeet has licensed its technology and patents to others, in some instances through enforcing its patents in litigation and in other instances through entering non-litigation licenses.

In the months prior to filing the current litigation, Plaintiff and its counsel performed a thorough pre-suit investigation to determine that the accused McAfee products infringe the asserted claims of the '559 Patent. The investigation included reviewing the '559 patent and its file history. Kajeet and its counsel have litigated the asserted claims in prior cases and have remained consistent in its view of the claims. They have been applied in Kajeet's investigation of McAfee products in a manner consistent with prior litigations. Plaintiff and its counsel reviewed publicly available information related to McAfee's Safe Family product and others that include the same parental control features. The information reviewed included a number of publicly available user guides, product specifications and videos authored by McAfee and others. Plaintiff compared the information related to the McAfee products with the asserted claims of the '559 patent and determined that each product infringed. Kajeet and its counsel prepared a claim chart with cites to the publicly available information showing how each product infringes. This analysis is reflected in part in Kajeet's complaints in this matter as well as in its Preliminary Infringement Contentions.

## IV. **LEGAL STANDARDS**

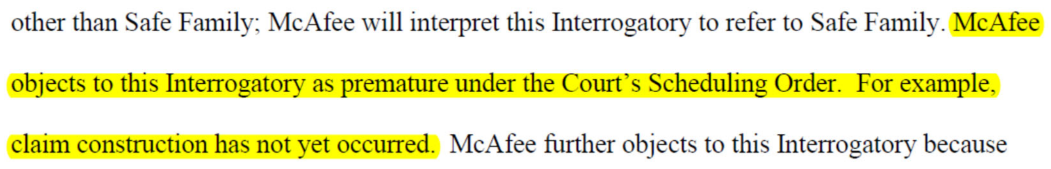
Rule 11 imposes upon attorneys a duty to certify that they have read any pleadings or motions they file and that they are well-grounded in fact, have a colorable basis in law, and are not filed for an improper purpose. Fed. R. Civ. P. 11(b); *Business Guides, Inc. v. Chromatic Comm. Enters., Inc*., 498 U.S. 533, 542 (1991); *View Eng'g v. Robotic Vision Sys.*, 208 F.3d 981, 984 (Fed. Cir. 2000). "[T]he imposition of a Rule 11 sanction is not a judgment on the merits of an action. Rather, it requires the determination of a collateral issue: whether the attorney has abused the judicial process, and, if so, what sanction would be appropriate." *Cooter & Gell v. Hartmarx*, 496 U.S. 384, 396 (1990). Courts consider factual questions relating to the extent of the attorney's pre-filing investigation and the bases underpinning the legal positions taken in a pleading when deciding whether to impose sanctions. *Cooter*, 496 U.S. at 399. Courts are cautioned to avoid viewing an attorney's actions with the benefit of hindsight and, instead, "test the conduct by inquiring what was reasonable to believe at the time the pleading, motion, or other paper was submitted." Fed. R. Civ. P. 11 Advisory Comm. Notes (1993 Amendments).

Regional circuit law controls Rule 11 motions in patent infringement cases. *ResQNet.com, Inc. v. Lansa, Inc*., 594 F.3d 860, 873 (Fed. Cir. 2010). Third Circuit law imposes an extremely high burden for proving a Rule 11 violation. Sanctions are applied only "in the 'exceptional circumstance' where a claim or motion is patently unmeritorious or frivolous." *Doering v. Union County Bd. of Chosen Freeholders*, 857 F.2d 191, 194 (3d Cir. 1988). The standard is whether counsel made a "reasonable inquiry into both the facts and the law supporting a particular pleading" to ensure it is well-grounded. *Schering Corp. v. Vitarine Pharms., Inc*., 889 F.2d 490, 496 (3d Cir. 1989). This reasonableness standard is "reasonableness under the circumstances, with reasonableness defined as an objective knowledge or belief at the time of the filing … that the claim was well-grounded in law and fact." *Ford Motor Co. v. Summit Motor Prods., Inc.*, 930 F.2d 277, 289 (3d Cir. 1991). The duty of "reasonable inquiry" is by no means a requirement "that pre-suit investigation into the facts be carried to the point of absolute certainty." *Forbes v. Eagleson*, 228 F.3d 471, 488 (3d Cir. 2000). The burden of proof and persuasion falls on the party moving for sanctions. *Tegg Corp. v. Beckstrom Elec. Co.*, 2008 U.S. Dist. LEXIS 100081, at *7 (W.D. Pa. Dec. 10, 2008) ("the burden of proof and persuasion rests on the party moving for sanctions"); *Rich Art Sign Co., Inc. v. Ring*, 122 F.R.D. 472, 474 (E.D. Pa. 1988) ("burden of proof on Rule 11 falls here on the defendants").

## V. ARGUMENT

### A. McAfee's Motion is Premature

At a minimum, McAfee's Motion is premature given the very early stage of this litigation and the limited amount of information that has been exchanged between the parties. McAfee served a copy of its Motion without waiting to receive Kajeet's infringement contentions which were due only a few weeks later and which demonstrate why McAfee's assertions are incorrect. McAfee made it clear in its recent interrogatory responses that it is simply too early in the case to evaluate the assertions it made in its Motion. In response to Kajeet's Interrogatory No. 1 seeking the factual basis for its non-infringement positions, McAfee objected:



other than Safe Family; McAfee will interpret this Interrogatory to refer to Safe Family. McAfee objects to this Interrogatory as premature under the Court's Scheduling Order. For example, claim construction has not yet occurred. McAfee further objects to this Interrogatory because

Exh. 3 at 7 (highlighting added)[2]. If McAfee cannot provide the basis for its non-infringement

[2] All Exhibit cites made herein are to those attached to the Declaration of Corby R. Vowell, filed concurrently herewith.

positions at this stage of the case, then how is the Court expected to properly consider the issues raised in the Motion and dismiss it with prejudice?

McAfee's refusal to provide meaningful technical documents on a timely basis is another reason why its Motion is premature. According to the Scheduling Order, McAfee was to have provided its core technical documents for the accused products on July 1, 2021. D.I. 22, at 4. McAfee's production was limited to a total of 22 pages of information and did not include any typical internal design documents that describe the architecture and operation of the accused products, such as technical specifications, requirements documents, software specifications, or other functional specifications. Vowell Decl. at ¶ 4. McAfee's scant production includes almost no information relevant to the design of the accused products, and certainly contained no internal technical information that could be used to confirm Kajeet's infringement positions or verify McAfee's baseless claims. On July 7, 2021, Kajeet's counsel sent a letter to McAfee describing the categories of documents that McAfee should have produced related to the accused products. Vowell Decl. at ¶ 4; Exhs. A, B. In its response, McAfee refused to provide these other technical documents and instead said that it would only provide access to its source code. *Id.*

McAfee then doubled down on its refusal to produce relevant technical information. Kajeet served interrogatories and document requests on McAfee on July 27, 2021 seeking *inter alia* the technical documents and information McAfee maintains and has for the accused products. Vowell Decl. at ¶ 5; Exh. C. McAfee served its responses to both on August 26, 2021, yet McAfee produced no documents along with those responses. *Id.*; Exh. D. After an inquiry to McAfee's counsel about its discovery responses, the parties held a meet and confer to discuss on August 31, 2021. McAfee's counsel made it clear that it would not be produce any documents in the next couple of weeks and instead would wait until approximately 4-6 weeks later to provide the bulk of its documents including the technical information that is highly relevant to this Motion. Vowell Decl. at ¶ 5.

McAfee likewise provided incomplete responses to the interrogatories. Specifically, McAfee responded, in part, to the interrogatory regarding its non-infringement positions that responsive information could be found in its source code. Yet, McAfee did not comply with Rule 33(d) and point to the specific portions or modules of the source code that were actually responsive to the interrogatory. Vowell Decl. at ¶ 7; Exhs. C, G, H. Kajeet immediately requested that McAfee do so, and during a meet and confer on this issue, McAfee's counsel stated that it would not identify which portions of the source code were relevant. Exh. H.

Further, McAfee took no discovery in this case prior to serving a copy of its Rule 11 Motion. It did not serve interrogatories or take depositions related to the veracity of Kajeet's infringement assertions. Indeed, McAfee very recently received Kajeet's infringement contentions and served a copy of the Motion well before reviewing them.

At this point, all McAfee can point to as Rule 11 violations are bald assertions based on no evidence. Ultimately, the non-infringement issues raised by McAfee are questions for the Court and jury to be decided on a more developed record. McAfee cannot cut off discovery and claim construction, simply because it disagrees with Kajeet's positions. *See Gaiardo v. Ethyl Corp.*, 835 F.2d 479, 483 (3d Cir. 1987) ("We caution litigants that Rule 11 is not to be used routinely when the parties disagree about the correct resolution of a matter in litigation."). Given the current state of the record, there is no basis to find that Kajeet violated Rule 11.

### B. Kajeet Conducted a Sufficient Pre-Suit Investigation

A reasonable and competent pre-filing inquiry entails "at a minimum, that an attorney interpret the asserted patent claims and compare the accused device with those claims before filing a claim alleging infringement." *Q-Pharma, Inc. v. Andrew Jergens Company*, 360 F.3d 1295, 1300-01 (Fed. Cir. 2004); *see also MEMC Elec. Materials v. Mitsubishi Materials Silicon Corp.*, 2004 U.S. Dist. LEXIS 29354, at *9-10 (N.D. Cal. July 9, 2004). There is no requirement to obtain the accused product to perform reverse engineering analysis. *GN Resound A/S v. Callpod, Inc.*, 2013 U.S. Dist. LEXIS 142822, at *11 (N.D. Cal. Sep. 27, 2013) (citing *Intamin, Ltd. Magnetar Techs. Corp.*, 483 F.3d 1328, 1338 (Fed. Cir. 2007) (no blanket rule requiring reverse engineering of accused product)).

Kajeet and its attorneys investigated the '559 patent and its file history to understand the meaning of the asserted claims and then applied the asserted claims to the accused products. Kajeet and its counsel reviewed product literature, manuals, and videos published by McAfee describing the components and functionality of the accused products. District courts have consistently held that such activities constitute an adequate pre-filing investigation of patent infringement claims. *See, e.g.*, *Mad Dogg Ath., Inc. v. Fitness Master, Inc.*, 2015 U.S. Dist. LEXIS 134942 at *5-8 (C.D. Cal. September 28, 2015).

In *Q-Pharma*, the Federal Circuit affirmed a denial of sanctions based on an allegedly inadequate pre-filing investigation. The Federal Circuit rejected defendant's argument that plaintiff's reliance on advertising material was not adequate to satisfy the requirements of Rule 11, even in light of the fact that the plaintiff could have directly analyzed the accused products for infringement. In its opinion, the Federal Circuit explicitly stated that such analysis was not required. *Q-Pharma*, 360 F.3d at 1302 ("While it is true that Q-Pharma could have conducted a more thorough investigation before filing suit, we conclude that its pre-filing infringement analysis was supported by a sufficient evidentiary basis. Q-Pharma acquired a sample of the Curel (R) CoQ[10] lotion and reviewed its advertising and labeling, which listed the product's ingredients and repeatedly touted the therapeutic effects of CoQ[10].").

Courts, including this Court, have found as sufficient pre-filing investigations that were less thorough than Kajeet's. See *Antonious v. Spalding & Evenflo Cos.*, 275 F.3d 1066, 1072-73 (Fed. Cir. 2002) (reversing sanctions under Rule 11(b)(2) because counsel "independently construed the patent claims before filing suit" and the construction was not frivolous); *Prism Techs. LLC v. Verisign, Inc.*, 579 F. Supp. 2d 625, 628 (D. Del. 2008). In *Prism*, for instance, counsel "analyz[ed] [the patent-in-suit] and determin[ed] whether certain … products … infringe[d] [,] developed detailed claim charts that analyzed [the] infringing products on an element-by-element basis[,] [and] obtained numerous manuals, guides and other documentation regarding the functionality of the … products …." *Prism Techs. LLC,* 579 F. Supp. 2d at 628. Based on that record, this Court held that counsel's "pre-filing investigation was adequate to support [its] claims of infringement …." *Id.* Kajeet and its counsel's pre-filing investigation at least included the steps taken in *Prism*.

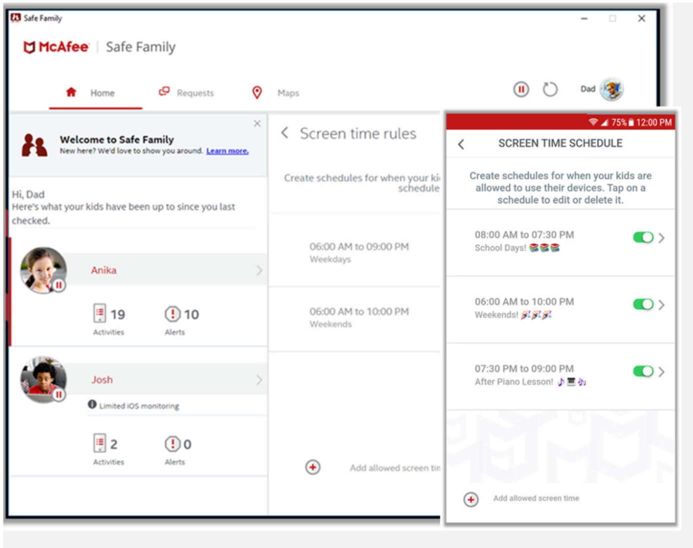
Kajeet's counsel reviewed product literature describing operation of the Accused Products as well as third party articles reviewing the same. These documents showed that the Accused Products effect similar functionality using a combination of hardware and software elements consistent with the many other parental control products that Kajeet has accused of infringement in prior litigations. Namely, the Accused Products effect policy-based control based on screen time / scheduling rules, among others, through implementation of local agent software on a controlled device communicating with a server backend. Sharma at ¶30.[3]

[3] In connection with this Response, Kajeet offers for submission a declaration from its technical expert, Mr. Chetan Sharma, which investigates and provides opinions on the operation of the Accused Products. Because this information presents expert opinion well before it is required pursuant to the schedule in this case, Kajeet hereby tenders Mr. Sharma's declaration for *in camera* inspection via delivery of it to the Court's chambers, in lieu of filing. *Acceleration Bay LLC v.*

Product literature describing the operation of the accused products shows that parents can update policies via an application using a parent's device (i.e., phone, tablet, or computer) accessing McAfee's servers. Sharma at ¶29. For example, in the screen capture below, "Dad" is logged in and able to view the profiles for two children. "Dad" has the ability through this portal to access logged activity for each child which is collected from the child's respective device(s) and logged on McAfee's servers for access by the parent. "Dad" may also see the policies applied ("Screen time rules"), which may be modified, toggled on/off, or to which additional policies may be added. This provides a reasonable basis for concluding that policies applied to manage the child device(s) are set and stored on McAfee's servers by an administrator, or parent. Mr. Sharma agrees. *Id.*

*Activision Blizzard, Inc.*, 2017 WL 9833512, at *1–2 (D. Del. 2017). Otherwise, McAfee will unjustly benefit from its effort to disrupt the case schedule and prematurely obtain expert discovery. Additionally, a Second Declaration of Corby R. Vowell is offered for submission for *in camera* inspection, which discusses the pre-suit diligence undertaken by Kajeet's counsel ahead of filing its original Complaint in this lawsuit. Of course, if the Court prefers that these declarations be filed, Kajeet will do so.

Kajeet will also tender for *in camera* inspection documents gathered and prepared by it as part of its pre-suit investigation, to include a claim chart and supporting documentation if desired by the Court. It is Kajeet's intention to preserve, and not waive in any way, work product privilege relating to its pre-suit diligence.



Welcome to Safe Family
New here? We'd love to show you around. Learn more.

Hi, Dad
Here's what your kids have been up to since you last checked.

Anika
19 Activities
10 Alerts

Josh
Limited iOS monitoring
2 Activities
0 Alerts

Screen time rules

Create schedules for when your ki
schedule

06:00 AM to 09:00 PM
Weekdays

06:00 AM to 10:00 PM
Weekends

Add allowed screen tin

75% 12:00 PM

SCREEN TIME SCHEDULE

Create schedules for when your kids are allowed to use their devices. Tap on a schedule to edit or delete it.

08:00 AM to 07:30 PM
School Days!

06:00 AM to 10:00 PM
Weekends!

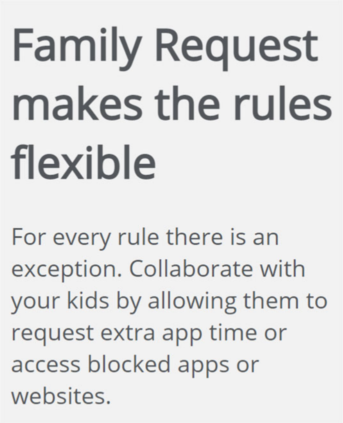
07:30 PM to 09:00 PM
After Piano Lesson!

Add allowed screen time

Exh. I at 3

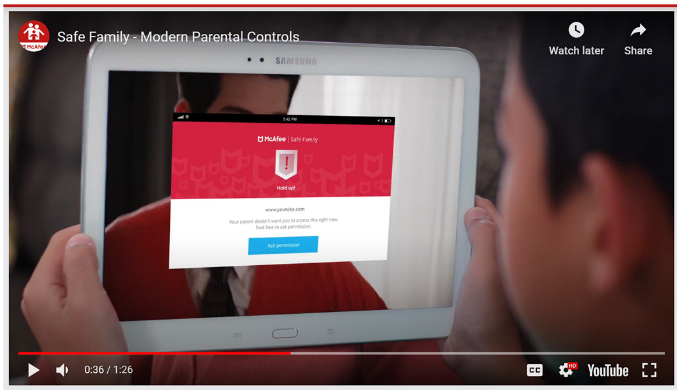
This is true regardless of the child's device being used during initial registration to configure policies. Use of the child's device at initial set up effects authentication of that device with the McAfee servers to allow for future communications therebetween. The child device serves merely as the portal for accessing McAfee's servers to set the master policies. This is evident from the Accused Products accommodating updates to the master policies being made by the parent through a parent device using the Safe Family application, rather than through the child's device. Sharma at ¶29-30.

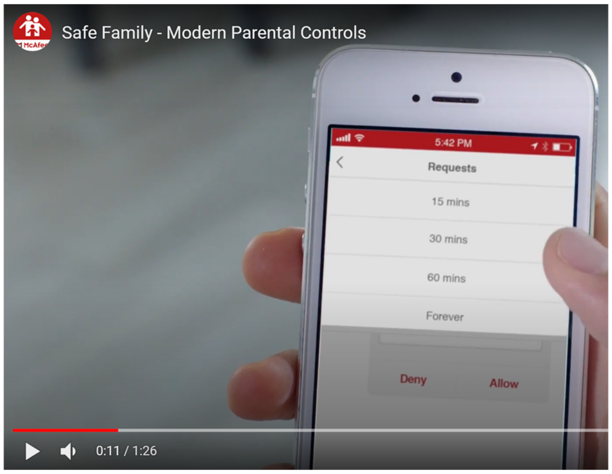
The accused products also provide for ad hoc updates to the policies applied in the form of requested exceptions, as shown below:



Family Request makes the rules flexible

For every rule there is an exception. Collaborate with your kids by allowing them to request extra app time or access blocked apps or websites.


Safe Family - Modern Parental Controls
Watch later
Share
SAMSUNG
McAfee | Safe Family
Hold up!
www.youtube.com
Your parent doesn't want you to access this right now.
Feel free to ask permission.
Ask permission
0:36 / 1:26
YouTube

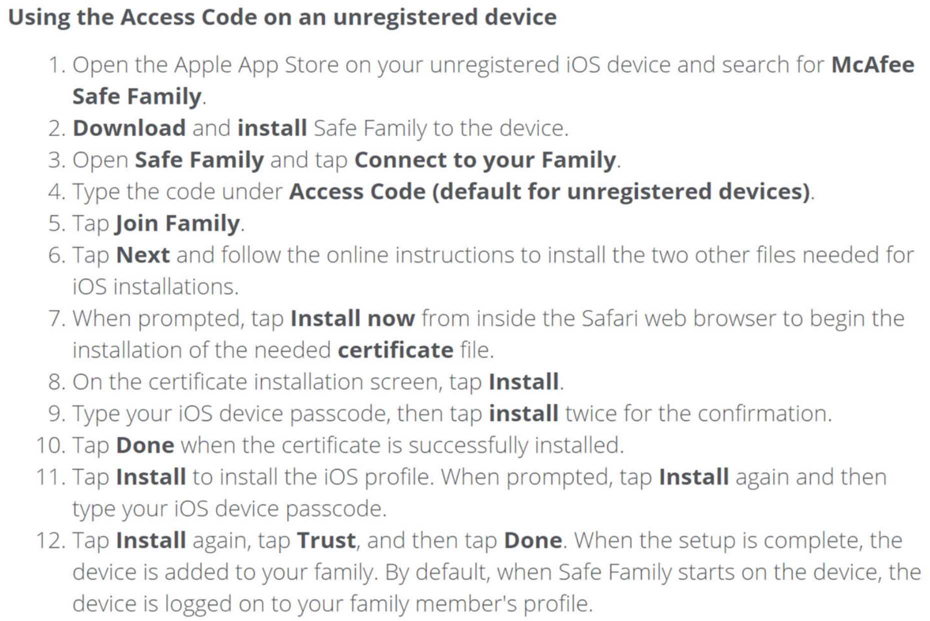


Exh. I at 1 (video), 4

The videos from which these screen captures were taken describe how the accused products operate to block impermissible uses of a child's device in real-time and in accordance with pre-defined policies set by a parent. Sharma at ¶30. They also demonstrate the ability of the child to request an exception to the policies applied in response to being blocked from performing some function. In this scenario, the child "requests" additional screen time. The parent may grant or deny that "request" using the parent's device, which then results in what McAfee's product videos show as an instantaneous update to the policies enforceable on the child device. Sharma at ¶30.

These communications are made through the McAfee Safe Family application resident on the parent and child devices, respectively, and are routed through McAfee's servers. Sharma at ¶30-31. The granting or denying of such "requests" shown in McAfee's product videos demonstrate, at a minimum, that real time decisions regarding device usage are made at the McAfee server and enforced on the child device. *Id.*

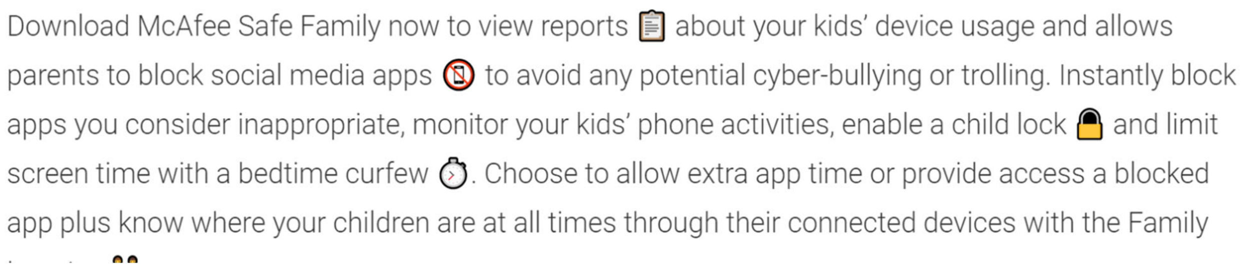
McAfee's product documentation further shows that during initial enrollment of a child device, certain certificates must be installed and permissions granted which indicate that the Accused Products maintain a continuous connection to McAfee's servers. For example, installation on an iOS device includes download of the Safe Family application, followed by "installation of the needed certificate file," an iOS profile, and designating Safe Family as trusted by the device. These operations are necessary to allow for communication with the Safe Family backend servers for transmission of requests and policy decisions, which are made via what McAfee itself describes as continuous communication between the child device and McAfee's servers. Sharma at ¶31-32.



**Using the Access Code on an unregistered device**

1. Open the Apple App Store on your unregistered iOS device and search for **McAfee Safe Family**.
2. **Download** and **install** Safe Family to the device.
3. Open **Safe Family** and tap **Connect to your Family**.
4. Type the code under **Access Code (default for unregistered devices)**.
5. Tap **Join Family**.
6. Tap **Next** and follow the online instructions to install the two other files needed for iOS installations.
7. When prompted, tap **Install now** from inside the Safari web browser to begin the installation of the needed **certificate** file.
8. On the certificate installation screen, tap **Install**.
9. Type your iOS device passcode, then tap **install** twice for the confirmation.
10. Tap **Done** when the certificate is successfully installed.
11. Tap **Install** to install the iOS profile. When prompted, tap **Install** again and then type your iOS device passcode.
12. Tap **Install** again, tap **Trust**, and then tap **Done**. When the setup is complete, the device is added to your family. By default, when Safe Family starts on the device, the device is logged on to your family member's profile.

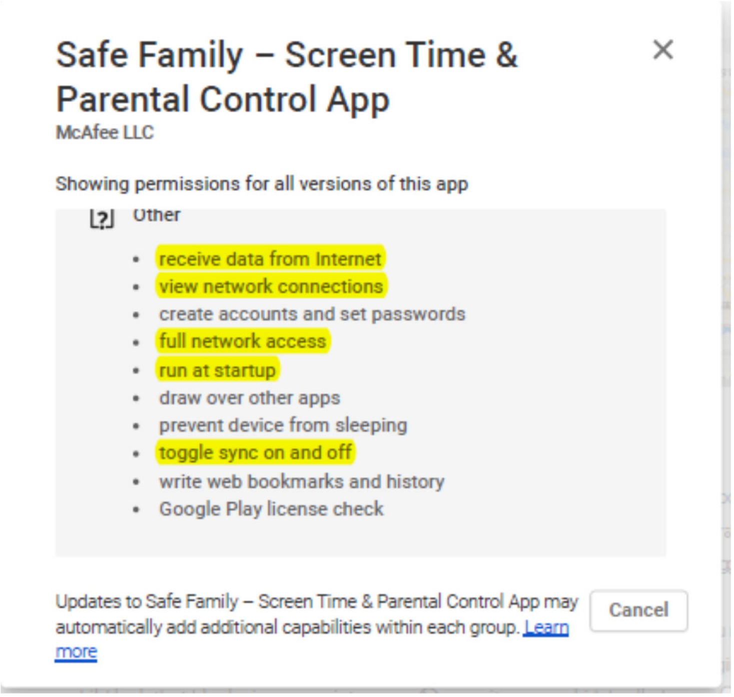
Exh. J at 3-4



Download McAfee Safe Family now to view reports 📋 about your kids' device usage and allows parents to block social media apps 📵 to avoid any potential cyber-bullying or trolling. Instantly block apps you consider inappropriate, monitor your kids' phone activities, enable a child lock 🔒 and limit screen time with a bedtime curfew ⏱. Choose to allow extra app time or provide access a blocked app plus know where your children are at all times through their connected devices with the Family

Exh. K at 1

Likewise, on Android devices, the Safe Family application requires permissions granting it access to receive data from the Internet, full network access, to run at startup of device, and to prevent the device from sleeping. These permissions are strongly indicative of the mobile application maintaining a network connection to McAfee's servers for the transmission and receipt of requests and policy decisions.



Safe Family – Screen Time & Parental Control App

McAfee LLC

Showing permissions for all versions of this app

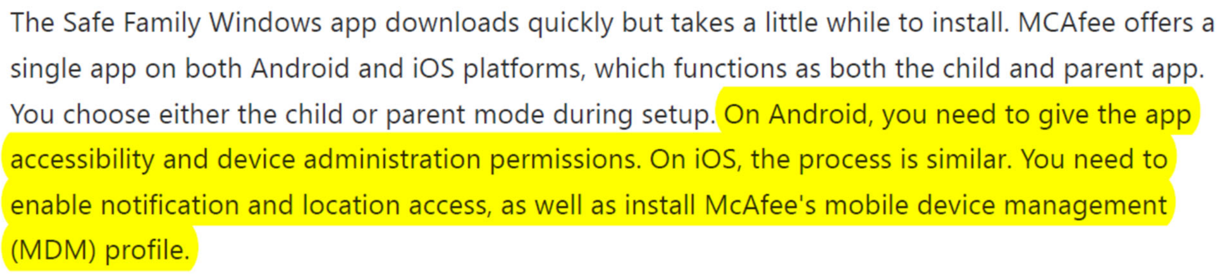
[?] Other

- receive data from Internet
- view network connections
- create accounts and set passwords
- full network access
- run at startup
- draw over other apps
- prevent device from sleeping
- toggle sync on and off
- write web bookmarks and history
- Google Play license check

Updates to Safe Family – Screen Time & Parental Control App may automatically add additional capabilities within each group. Learn more

Exh. L (highlighting added)

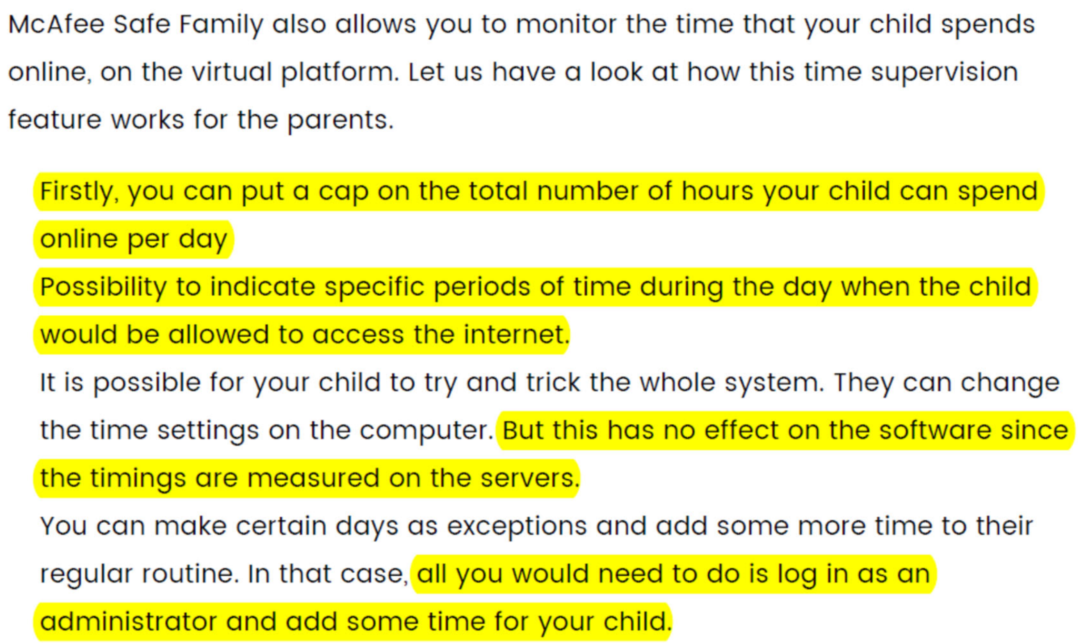
Product reviews for the Accused Products confirm the same and further describe operation of the Accused Products in manner consistent with Kajeet's infringement claims.



> The Safe Family Windows app downloads quickly but takes a little while to install. MCAfee offers a single app on both Android and iOS platforms, which functions as both the child and parent app. You choose either the child or parent mode during setup. On Android, you need to give the app accessibility and device administration permissions. On iOS, the process is similar. You need to enable notification and location access, as well as install McAfee's mobile device management (MDM) profile.

Exh. M (highlighting added) at 3

These articles, which are based upon product testing by the respective authors, affirm that using the Safe Family application parents can access real time information showing activity on the child device and its current location. Again, this real time information can only be available to the parent if the child device is in constant communication with the McAfee servers, which store master policies defining at least time / scheduling rules for device usage which are applied simultaneously to devices associated with a child's profile.



McAfee Safe Family also allows you to monitor the time that your child spends online, on the virtual platform. Let us have a look at how this time supervision feature works for the parents.

Firstly, you can put a cap on the total number of hours your child can spend online per day

Possibility to indicate specific periods of time during the day when the child would be allowed to access the internet.

It is possible for your child to try and trick the whole system. They can change the time settings on the computer. But this has no effect on the software since the timings are measured on the servers.

You can make certain days as exceptions and add some more time to their regular routine. In that case, all you would need to do is log in as an administrator and add some time for your child.

Exh. N (highlighting added) at 4

The evidence considered by Kajeet as part of its pre-suit investigation therefore provided a reasonable basis for concluding that the Accused Products utilize the request-decide-enforce control methodology required by the asserted claims, with master policies residing on McAfee's servers.

Kajeet's reasonable basis for asserting infringement by the Safe Family products is bolstered by its counsel's experience gained from prior litigations enforcing the '559 Patent. Kajeet has asserted infringement of claims of the '559 Patent against several infringers over the past few years, many of whom offer products accommodating virtually identical functionality to manage the use of a child's (or employee's) mobile device as Safe Family. Through these litigations, Kajeet's counsel has learned about the typical operation of such products in accordance with commonly encountered implementations, such as through the use of application software acting as a local agent on the managed device in combination with a remote server storing master policies. This is the precise component arrangement utilized by the Safe Family product which is used to effect similar or identical types of control that Kajeet has encountered in prior litigations.

This acquired knowledge base in combination with the statements made and functionality shown in publicly available documents and videos addressed to operation of the Safe Family product more than justify Kajeet in bringing this lawsuit.

### C. Kajeet Has a Reasonable Basis for Maintaining Its Case

McAfee contends that Kajeet has no reasonable basis for maintaining its infringement claims against the Safe Family product because, according to McAfee's attorneys, the application continues to effect some control over a child device even at times when the child device is not able to communicate with McAfee's remote servers. McAfee contends that policies must be stored on the child device, therefore, and that communication with a server is not required for operation of the Safe Family product. This is an unsupported strawman argument that is premised upon application of claim constructions not entered in this case and upon unsupported conclusions.

First, McAfee's contention rests upon its failure to account for the necessary differences in meaning between several claim terms, including at least constructions for a "decision" that is received by the computing device from the server and for "a policy" that is stored at the server. McAfee's arguments do not treat these elements as two separate requirements of the claim and appears to, instead, conflate them into a single requirement of the asserted claims. In other words, McAfee's argument is premised upon the incorrect notion that if ***anything*** is stored on the computing device that may be consulted to enforce parental controls, then the language of the asserted claims cannot be met. This is not what the claims require, however. This skewed interpretation is much narrower than the claim language expressly requires.[4]

Second, McAfee erroneously presents the conclusion that some continued control even when the device cannot communicate with a server ***necessarily*** means that policies must be stored on the child device. This is not necessarily so, however. A more likely manner of operation that would accommodate some continued offline enforcement would be for the child device to store the most recent ***decisions*** received from the server for similar requests made at an earlier time when communication with the server was available.[5] Put another way, if the last time a request to the server resulted in decision to not allow a particular action, then next time that action was requested the device would attempt to query the server and, if unable to do so, would continue to apply the previously received "block" decision. This manner of operation does not offend any limitation of the asserted claims, which are silent as to the local storage of decisions. Further, this manner of operation is expressly claimed in other claims of the '559 Patent, such as Claim 13.

Third, to the extent McAfee's contention could have any merit for demonstrating noninfringement, it has not been supported by competent evidence. Several types of policies effecting different controls over a child device are accused of infringement. Additionally, operation of the Safe Family product in connection with several different types of devices implemented with different operating systems are accused. McAfee makes no attempt to address each of the policy types as applied to each of the different operating systems Kajeet has accused.

[4] Additionally, wholesale adoption of McAfee's interpretation at this stage effectively forecloses Kajeet from asserting infringement under the Doctrine of Equivalents. A key aspect of the asserted claims is the application of decisions that are ***based on*** a policy stored at a server to control a computing device. It is possible that this is achieved despite there being insubstantial differences between characteristics of an accused product and the precise language of the asserted claims.

[5] The actual and complete operation of the Accused Products will eventually be revealed when McAfee belatedly makes a fulsome document production and/or when Kajeet is able to complete its inspection of the source code.

Instead, McAfee's counsel provides generic and unsupported attorney argument purporting to describe operation of the Safe Family product without any accounting for these various implementations[6] and yet, unbelievably, expects that Kajeet would dismiss its claims of infringement in their entirety in response.

Lastly, McAfee's argument centers only on the operation of the Safe Family products when not in its intended operating state or, stated differently, when they are in a non-functional mode of operation. To be sure, Safe Family is intended to be used with ***connected*** devices to, among other functionality, continuously inform the parent of the device's location and how it is being used while also enforcing the current master policies stored at the McAfee servers. When unconnected, the devices cannot perform any of these functions. No activity or location reporting is possible. Likewise, any changes or updates to policies made by a parent will not be enforced on the child device. In this mode, Safe Family fails to provide any utility. Further, this mode of operation is entirely outside of the scope of the asserted claims, each of which require that the controlled device be connected to a communication network. Operations when not connected are immaterial, therefore.

Despite these glaring holes in McAfee's noninfringement argument, Kajeet has nonetheless diligently undertaken to review all information and materials available to it showing operation of the Safe Family products to ascertain the veracity of McAfee's arguments. This includes consultation with an expert in the field, review of McAfee's scant document production, inspection of source code for Safe Family products, product testing on Android, iOS, and Windows devices, and use of the WireShark packet sniffing software. This analysis showed McAfee's

[6] Notably, despite its assertions as to how the accused products operate, McAfee has refused to identify any source code or product documentation in support of its noninfringement positions in its response to Kajeet's discovery requests. Vowell Decl. at ¶7.

arguments to be unavailing and that Kajeet's infringement position has merit.

Briefly, Kajeet's continued investigation into the operation of the Accused Products indicates that they: (1) implement master policies that are stored on McAfee's servers (or "backend"); (2) cause controlled devices to direct communications through McAfee's servers; (3) McAfee's server acts as an intermediary between input received from a parent device and subsequent enforcement on a child device; (3) regular communication between the child device and McAfee's server are necessary for the Accused Product to operate as intended; and, (4) at least some of these communication are triggered by attempted use of the computing device by a child, as confirmed by testing, source code inspection, and use of WireShark. These topics and evidentiary support for each are discussed in detail in the Sharma Declaration. Sharma at ¶17-30.

The evidence accessible and inspected by Kajeet in this litigation, to date, fails to indicate that Kajeet's infringement position is incorrect. Rather, the evidence confirms Kajeet's ongoing reasonable basis for continuing in discovery and maintaining its infringement claims.

## VI. CONCLUSION

For the reasons set forth above, McAfee's Motion should be denied in its entirety.

Dated: September 7, 2021

Of Counsel:

Jonathan T. Suder
Michael T. Cooke
Corby R. Vowell
Richard A. Wojcio, Jr.
FRIEDMAN, SUDER & COOKE
Tindall Square Warehouse No. 1
604 East 4th Street, Suite 200
Fort Worth, Texas 76102
Telephone: (817) 334-0400
Facsimile: (817) 334-0401

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan
Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market Str., 12th Floor
Wilmington, DE 19801
Tel: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

| | |
|---|---|
| jts@fsclaw.com<br>mtc@fsclaw.com<br>vowell@fsclaw.com<br>wojcio@fsclaw.com | *Attorneys for Plaintiff Kajeet, Inc.* |